Ciencia e Ingeniería
Revista Interdisciplinar de Estudios en Ciencias Básicas e Ingenierías.
Año 2016, Enero-Junio, Vol. (3) N° (1) ISSN 2389-9484.
Universidad de La Guajira, Facultades de Ciencias Básicas y Aplicadas e Ingeniería.
La Guajira-Colombia.
Revista en Línea http://revistas.uniguajira.edu.co/index.php/cei



GESTIÓN SEGURA DE LA INFORMACIÓN. COMPETENCIA GENÉRICA CLAVE EN UNA SOCIEDAD DE LA INFORMACIÓN Y EL CONOCIMIENTO

SAFE INFORMATION MANAGEMENT. GENERIC COMPETITION ON A KEY INFORMATION SOCIETY AND KNOWLEDGE

Jeimy J. Cano M.

Universidad Santo Tomás de Aquino
jjcano@yahoo.com

Recibido: Agosto 21 de 2015 Aceptado: Febrero 11 de 2016

RESUMEN

La información en la sociedad de la información y el conocimiento es un activo estratégico de las empresas del siglo XXI y su inadecuado tratamiento por parte de los individuos ocasiona brechas de seguridad de la información que generan implicaciones serias para las organizaciones expresadas generalmente en pérdidas económicas, sanciones legales y pérdida de reputación. En razón a lo anterior, comprender los retos prácticos y estructurales de la custodia de la información como activo estratégico desde la perspectiva de las competencias genéricas, nos permiten reconceptualizar los avances y estudios previos centrados en la competencia digital y el tratamiento de la información, para fundar una propuesta de competencia genérica en gestión segura de la información. Este estudio adopta un discurso epistemológico basado en el pensamiento de sistemas para comprender cómo se desarrolla y construye la cultura organizacional de seguridad de la información (COSI). Con estos fundamentos, se delinea una propuesta de competencia genérica en gestión segura de la información que detalla los comportamientos claves esperados de los individuos, así como algunos indicadores base de cada uno de ellos para establecer su nivel de dominio, enmarcados en un enfoque socioformativo que entiende la formación como un proceso sistémico de corresponsabilidad entre la persona y su entorno

Palabras Clave: Sociedad de la información y el conocimiento, competencias genéricas, competencia digital y tratamiento de la información, gestión segura de la información, pensamiento de sistemas

ABSTRACT

The information in the knowledge and information society is a strategic asset of enterprises in the XXI century and its inadequate treatment by individuals brings security breaches of the information generated serious implications for organizations usually expressed in economic losses, legal penalties and loss of reputation. Due to the above, understand the practical and structural challenges of custody of information as a strategic asset, from the perspective of generic competencies allow us to reconceptualize the progress and previous studies focused on digital competence and treatment of information, to establish a proposed generic competency in information security management. This study adopts an epistemological discourse based on systems thinking to understand how it develops and builds organizational culture of information security (COSI). With these fundamentals, a proposed generic competency in information security management detailing the key behaviors expected of individuals, as well as some indicators base of each one of them to establish their level domain, surrounded by a socioformative approach is outlined that understands training as a systemic process of co-responsibility between the person and their environment.

Keywords: knowledge and Information society, generic competencies, digital competence and information processing, information security management, systems thinking

1. CULTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN: VISTA SISTÉMICA DE LA CULTURA DE SEGURIDAD DE LA INFORMACIÓN

Reid, Van Nieker y Renaud (2014) introducen el concepto de cultura de seguridad de la información, entendiendo éste desde la vista de sistemas anidados que revelan propiedades emergentes que le permiten automantenerse y autorepararse. Esta lectura corresponde a una interpretación desde la teoría de los sistemas vivos, los cuales son entes abiertos, complejos, adaptativos y autoorganizados que interactúan con su medio ambiente u otros sistemas.

Esta definición introduce la noción de anidamiento, que leído en términos cibernéticos (Hoverstadt, 2008), significa establecer un patrón orgánico que se repite al interior de la estructura estudiada, en donde el nivel superior depende de los comportamientos propios de los niveles inferiores. Esto supone comprender que cada interacción entre los participantes de un grupo particular y contexto específico, logra construir una vista propia de actuación que marca una forma y proceso que la distingue, sin perjuicio que comparta la generalidad presente en el nivel estudiado.

Cuando empezamos la revisión desde el nivel general y vamos a niveles particulares, el ejercicio que se realiza es de análisis, lo cual permite conocer y descubrir la estructura en la cual nos movemos para advertir los componentes de la cultura organizacional de seguridad de la información (COSI). Mientras al regresarnos del nivel inferior al superior, adelantamos diagnóstico del nivel superior, basado en las reflexiones y revisiones efectuadas en el nivel inferior. De esta forma confirmamos la vista sistémica de la estrategia para conocer la COSI como se observa en la figura 1.

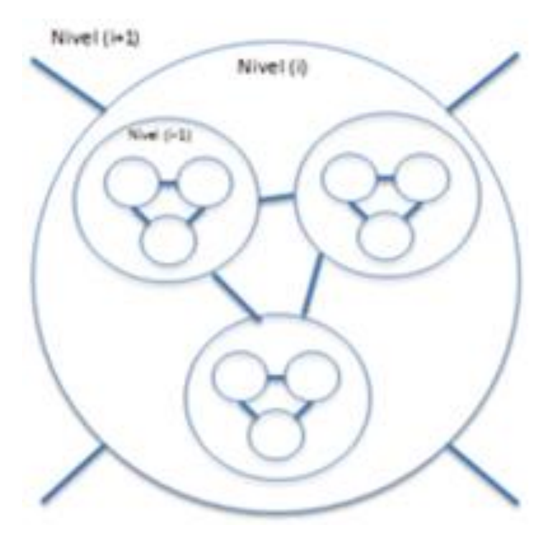


Figura 1. Vista anidada de la construcción y diagnóstico de una cultura organizacional de seguridad de la información (Adaptado de: Reyes 1995, cap.5)

En consecuencia, en este ejercicio sistémico cibernético, la complejidad inherente de la cultura organizacional de seguridad de la información, se va asumiendo de manera paulatina por la revelación y análisis de los patrones identificados, basados en los tres elementos claves enunciados por Alnatheer (2012), apropiación, concientización y cumplimiento, los cuales le dan forma y respuesta a la pregunta: ¿cómo se construye y desarrolla una cultura organizacional de seguridad de la información?

2. COMPETENCIA GENÉRICA DE GESTIÓN SEGURA DE LA INFORMACIÓN

Fundados en los supuestos del enfoque socioformativo de competencias, se define la competencia genérica de gestión segura de la información como la que adquiere un individuo cuando:

Gestiona el tratamiento de la información personal y empresarial para asegurar su adecuada protección, a través de un marco normativo y de buenas prácticas reconocidas, considerando y entendiendo el escenario de riesgos definido en un contexto particular.

Esta competencia genérica está definida por tres competencias claves, referidas a los elementos que definen una cultura de seguridad de la información expuestos por Alnatheer (2012):

- Competencia de apropiación de la seguridad de la información
- Competencia de concientización en seguridad de la información
- Competencia de cumplimiento en seguridad de la información

Cada una de ellas, es complementaria entre sí y se alimenta de la evolución de la otra, de tal forma que alcanzar un nivel de dominio de la competencia genérica, demanda un aseguramiento de cada una de ésta competencias clave enunciadas. Así las cosas, se ofrecen las definiciones adicionales que desglosan cada ellas y sus criterios de evolución para alcanzar su perfeccionamiento.

A. Competencia de apropiación de la seguridad de la información

Definición:

Comprende los riesgos e impactos del tratamiento de la información para asegurar las prácticas y procedimientos de protección requeridas, considerando las herramientas y técnicas disponibles en la organización.

Criterios: (1 equivale a nivel básico y 3 al nivel avanzado)

A.1 Conoce y analiza los riesgos e impactos del tratamiento de la información en el desarrollo de sus actividades en la organización, de acuerdo con el marco normativo vigente.

A.2 Decide y actúa de acuerdo con la comprensión de los riesgos e impactos en el tratamiento de la información en el desarrollo de sus actividades en la organización, de acuerdo con el marco normativo vigente.

A.3 Aplica y promueve las acciones de protección requeridas para asegurar el adecuado tratamiento de la información considerando las herramientas y técnicas disponibles en la organización.

B. Competencia de concientización en seguridad de la información
Definición: *Asume las consecuencias de sus acciones respecto del tratamiento de la información para asegurar los beneficios de la aplicación de las prácticas de protección definidas y requeridas y el reporte de desviaciones y fallas que se presenten, considerando el escenario de riesgos y controles establecido en la organización.* **Criterios:** (1 equivale a nivel básico y 3 al nivel avanzado) B.1 Conoce y acepta sus responsabilidades respecto del tratamiento de la información, de acuerdo con su rol, en el desarrollo de sus actividades diarias. B.2 Decide y actúa respecto del tratamiento de la información de acuerdo con la política de seguridad vigente. B.3 Reporta y asiste los procedimientos establecidos frente a las desviaciones y fallas en el tratamiento de la información, considerando el marco normativo y de buenas prácticas de seguridad de la información vigente.

C. Competencia de cumplimiento en seguridad de la información
Definición: *Cumple con el marco normativo y de buenas prácticas definido en el tratamiento de la información para asegurar su adecuada protección y así, resguardar la imagen y valor de la empresa, considerando el escenario de riesgos y controles definido por ésta.* **Criterios:** (1 equivale a nivel básico y 3 al nivel avanzado) C.1 Conoce y entiende el marco normativo de buenas prácticas definido en el tratamiento de la información en el desarrollo de su rol en la organización. C.2 Adhiere y actúa de acuerdo con las prácticas de seguridad y control definidas en el marco normativo de seguridad de la información. C.3 Ejecuta y sigue el marco normativo y de buenas prácticas de seguridad y control de acuerdo con el escenario de riesgos y controles definidos por la empresa.

Cada uno de los niveles expresados para cada competencia clave, establece un conjunto de indicadores que dan cuenta del avance en el dominio de ese criterio. En consecuencia y a manera de ilustración se describe a continuación el detalle de los indicadores previstos para el criterio A.1, que nos permite advertir el nivel de exigencia que demanda satisfacer dicho criterio, los cuales requieren, siguiendo el enfoque socioformativo de competencias, el problema del contexto, las pautas y aspectos clave de la formación y evaluación y sus evidencias (Tobón, 2013).

Problema de contexto: ¿Cómo enfrentarse a los retos del aseguramiento de la información, basado en los riesgos e impactos de su tratamiento, para apropiarse de las prácticas y procedimientos de protección requeridos, considerando las herramientas y técnicas disponibles en la organización?		
Criterio	**Indicadores**	**Evidencias**
A.1 Conoce y analiza los riesgos e impactos del tratamiento de la información en el desarrollo de sus actividades en la organización, de acuerdo con el marco normativo vigente.	1. Conoce los riesgos básicos de la seguridad de la información 2. Integra a sus actividades diarias los riesgos básicos de la seguridad de la información y sus impactos en la empresa. 3. Diferencia los riesgos e impactos de la seguridad de la información en sus actividades diarias. 4. Incorpora en su modelo mental los riesgos e impactos de la seguridad de la información en sus actividades diarias. 5. Demuestra capacidad para transferir los conocimientos teóricos y prácticos de los riesgos e impactos de la seguridad de la información	1. Registro de la observación de la persona validando los riesgos básicos de la seguridad de la información (pérdida y/o fuga de información, acceso no autorizado, suplantación, revelación de información no autorizada, manipulación de información) 2. Registro de la observación de la persona adelantando análisis de los riesgos básicos en seguridad de la información en al menos tres situaciones de trabajo. 3. Al menos la evidencia de tres charlas sobre análisis de riesgos en seguridad de la información en diferentes situaciones.

3. CONCLUSIONES

Si bien la competencia de tratamiento de la información y competencia digital es una iniciativa europea que se ha venido incorporando en muchos países del viejo continente a través de la recomendación del parlamento europeo y el Consejo de la Unión Europea - CUE (CUE, 2006), llamamos la atención de la implementación que se ha adelantado en España mediante la expedición de dos piezas legislativas de alcance nacional como los Reales Decretos 1513/2006 y 1631/2006 por las cuales se establecen ocho competencias básica, dentro de las cuales se hace referencia a la de tratamiento de la información y competencia digital.

Al comparar lo establecido por el CUE y la implementación desarrollada en España notamos que se establecen diferencias interesantes, que son relevantes para el contexto de la competencia de gestión segura de la información.

Consejo de la Unión Europea – CUE (2006) Sobre las competencias claves para el aprendizaje permanente – *Competencia digital*	Real Decreto 1513/2006 y 1631/2006 – Competencias básicas – *Tratamiento de la información y competencia digital*
Definición: La competencia digital entraña el uso seguro y crítico de las tecnologías de la sociedad de la información (TSI) para el trabajo, el ocio y la comunicación. Se sustenta en las competencias básicas en materia de TIC: el uso de ordenadores para obtener, evaluar, almacenar, producir, presentar e intercambiar información, y comunicarse y participar en redes de colaboración a través de Internet.	Definición: Disponer de habilidades para buscar, obtener, procesar y comunicar información, y para transformarla en conocimiento. Incorpora diferentes habilidades, que van desde el acceso a la información hasta su transmisión en distintos soportes una vez tratada, incluyendo la utilización de las tecnologías de la información y la comunicación como elemento esencial para informarse, aprender y comunicarse

Mientras la definición propia de la recomendación europea se requiere una actitud crítica y reflexiva respecto de la información para efectuar un uso seguro de la misma, en la definición española el énfasis se hace en la alfabetización informacional y tecnológica, como fundamento del saberse informar, aprender y comunicarse. En este sentido, la recomendación europea, ajustada a los términos de Ferrari (2013), particularmente en el área de seguridad, establece un referente conceptual base que anticipa la necesidad de formular una competencia genérica en gestión segura de la información, como condición base de la ciudadanía digital tanto de los actuales profesionales de las organizaciones, como de los nativos digitales.

En este sentido, se requiere fundamentar comportamientos básicos claves que permitan asegurar un adecuado tratamiento de la información, para lo cual las ideas de Alnatheer (2012) sobre aquellos elementos que definen la cultura de seguridad de la información se vuelven relevantes. La apropiación, la concientización y el cumplimiento, como componentes base de la competencia de gestión segura de la información establecen un conjunto concreto de comportamientos que permiten no solo dar cuenta de lo expuesto en la recomendación europea, sino que especifica concretamente cómo alcanzar el nivel requerido y las implicaciones que ello tiene en una organización.

Las implicaciones organizacionales del desarrollo de la competencia de gestión segura de la información se advierten en el contexto del modelo de madurez de cultura organizacional de seguridad de la información, como quiera que niveles bajo de desarrollo de la competencia, movilizarán a la empresa en tendencias reactiva e inestable, incrementando los niveles de exposición al riesgo de la organización respecto de la pérdida y/o fuga de la información.

Por tanto, motivar el desarrollo e implementación de una competencia genérica en gestión segura de la información, acelera la incorporación de prácticas y fundamentos éticos de actuación de las personas, como se advierte en la definición de competencias de Tobón (2013), los cuales trazan el camino para incrementar la resistencia de las organizaciones frente a fallas y vulnerabilidades planteadas alrededor de los

comportamientos de las personas, las cuales representan el eslabón más débil de la cadena en el ejercicio de aseguramiento de activos estratégicos de información.

En la medida que se avance en el perfeccionamiento de la competencia genérica en gestión segura de la información, ajustados a los fundamentos del enfoque socioformativo de competencias, se hará más evidente la corresponsabilidad de las actuaciones de los individuos frente al tratamiento de la información habida cuenta que sus acciones respecto del problema del contexto deberán ser idóneas y ajustadas al compromiso ético que reconoce al otro como verdadero otro, según establece Maturana (1998).

4. REFERENCIAS BIBLIOGRAFICAS

Alnatheer, M. (2012) *Understanding and measuring information security culture in developing countries: case of Saudi Arabia* (Doctoral Thesis). Queensland University of Technology, Australia.

Consejo de la Unión Europea – CUE (2006) Sobre las competencias claves para el aprendizaje permanente. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32006H0962

Ferrari, A. (2013) DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe. Recuperado de: http://is.jrc.ec.europa.eu/pages/EAP/DIGCOMP.html

Maturana, H. (1998) *Emociones y lenguaje en educación y política*. Dolmen Ediciones.

Reid, R., Van Niekerk, J. y Renaud, K. (2014) Information security culture: A general living systems theory perspective. *Information Security for South Africa* (ISSA), 13-14 August. 1-8. Doi: 10.1109/ISSA.2014.6950493.

Reyes, A. (1995). *A theoretical framework for the design of a social accounting system* (Doctoral Thesis). University of Humberside. United Kingdom.